

## **"This is what I'm thinking about...." A (Theoretical) Tactical Commander Gives His IO Guidance**

**by MAJ Matthew A. Stern and MAJ (Ret) Steven M. Seybert**

---

### **Introduction**

Experience has shown that the commander's initial guidance is absolutely critical to initiating the military decisionmaking process. The commander is called upon to provide guidance on every battlefield operating system (BOS), regardless of his expertise, or perhaps lack thereof. Likewise, it is critical that the commander provides guidance on the conduct of Information Operations (IO). Being a newcomer - at least in title - to the battlefield, however, IO may not get equal treatment in being addressed by the commander. Additionally, as the greater Army struggles to define IO doctrinally and operationally, commanders may feel less than comfortable in delving intellectually or operationally into the untried territory of IO guidance. What does a commander's IO guidance sound and look like? This article provides a few pointers on topics that a tactical commander may consider when developing initial IO planning guidance and a concrete example of that guidance. Additionally, a residual benefit of this article may be some sample applications of IO activities for tactical warfighting units.

The information contained in this article is based on **FM 100-6, *Information Operations***, and **FM 101-5, *Staff Organization and Operations***, and on personal experiences. FM 100-6 is the Army's doctrinal cornerstone for IO planning and execution. FM 101-5 provides the doctrinal perspective on guidance required of the commander for the seven elements of IO: electronic warfare (EW), psychological operations (PSYOP), physical destruction, operations security (OPSEC), deception, civil affairs (CA), and public affairs (PA).<sup>1</sup>

### **General**

The commander's initial IO guidance normally emerges from an information exchange between the commander and selected battle staff members, typically the G2, G3, G6, the fire support coordinator (FSCoord), and the unit's IO Officer. The G2, G3, FSCoord, and IO Officer help the commander visualize offensive IO requirements and opportunities. The G2, G6, and IO officer provide expertise on friendly vulnerabilities, enemy offensive IO capabilities, available technical protect measures, and potential defensive applications of friendly IO capabilities (defensive IO).<sup>2</sup>

The commander's intent must provide sufficient guidance for IO planning. The commander should state in finite and measurable terms any identified or contemplated IO objectives. These stated objectives and any resulting tasks must be tied directly to operational decision points to be operationally relevant.

In developing initial IO planning guidance, the commander should consider the following:

- Emphasizing courses of actions (COAs) in which employing IO enhances the likelihood of mission success.
- To what extent the unit is vulnerable to hostile IO.
- If there are specific offensive and defensive IO actions that are required for the operation.
- The unit's capability to execute the specific offensive IO actions and to implement specific defensive IO measures.
- Additional data on IO needed to plan or execute the operation. This data would fall in the category of the commander's critical information requirements (CCIRs), including essential elements of friendly information (EEFI), friendly forces information requirements (FFIRs), and priority intelligence requirements (PIRs).
- Acceptable risk in executing or not executing IO.
- Coordination requirements critical to conducting IO in the operation.
- Approval authorities to retain or delegate.
- Higher command policies and guidance.<sup>3</sup>

### **Required Guidance**

FM 101-5 specifies the general areas for all battlefield operating and coordinating functions requiring guidance from the commander. For IO, these areas are generally grouped under the seven different elements of IO.<sup>4</sup> Although the current edition of the FM does not identify specific guidance requirements for CA, the authors have taken the liberty of including our version of it since CA is an integral element of IO. For illustrative purposes only, the following guidance examples are written as if the commander was providing a full guidance statement for each IO element.

It is important to note that a commander normally would not have the time or the inclination to deal with each of these areas as extensively as done here: his concept and intent need to be short and very precise. The following are perhaps more of a reflection of what the commander and selected staff members might discuss as they attempt to understand the situation, combined with some of the deliberations the unit's IO Cell may sort through as it deals with planning details.

The important aspect of IO in integrating the various elements it comprises is not directly addressed in the FM and needs to be discussed before delving into the guidance for specific elements of IO. The current concept of IO is as an integrating function that focuses various capabilities and activities to achieve and retain an information advantage, whether dominance or superiority, over an adversary.<sup>5</sup> Although the following discussion is formatted by IO element, integration of the various elements is the most critical aspect of IO and is addressed throughout the discussion. More importantly, a broad IO guidance example is presented later in this article and demonstrates the overall integration essential for successful IO.

## **TACTICS, TECHNIQUES AND PROCEDURES (TTP)**

### **Military Deception**

Deception is designed to mislead the enemy by manipulation, distortion, or falsification of information to induce him to act in a way that is beneficial to friendly forces. There are three basic ways to use deception: to influence opposing commanders, to degrade enemy intelligence collection on friendly forces, and to protect units, systems, and soldiers from enemy weapons systems. These are referred to as Military Deception, Deception in support of OPSEC, and Deception as part of Camouflage, Concealment, and Deception (CCD), respectively. There are three key points related to conducting deception that we would like to highlight here. First, the best bet for a successful deception effort is one that reinforces what the enemy already believes or is inclined to believe: "Give him what he wants." Next, the deception effort must be sufficiently resourced such that it will be credible enough to withstand some level of enemy scrutiny. Last - and this is related to the previous point on resourcing - deception requires a significant amount of time to plan, execute, and assess.

**Possible deception mission statement:** "Attack southeast of OBJECTIVE HAWK to deceive the 20th Motorized Rifle Division (MRD) commander as to the actual intent and purpose of our unit's operations, thereby delaying commitment of his local counterattack force - the 204th Tank Regiment (TR) - for at least 4 hours."

**Amount and types of resources to commit to the deception plan:** "I will commit a brigade task force and the attack helicopter battalion to achieve our deception goal."

**Intent for exploiting enemy actions:** "My intent is to ensure we have sufficient time to defeat the forces on the objective and begin preparing our positions prior to facing the 20th MRD commander's heavy counterattack force."

**CCIR:** "We must confirm the location of the local counterattack force prior to being able to conduct this deception. We also must know that the enemy will have the capabilities to read our deception so tell me the status of his intelligence, surveillance, and reconnaissance (ISR) capabilities and decisionmaking process he will use to make that read. We must also know the status of our resources that will conduct and assess the deception operation. I must know at H+3 if the 20th MRD commander believes the deception story."

### **OPSEC Considerations**

OPSEC is key to denying the enemy information. Its goal is to selectively deny exploitable friendly information and indicators to the enemy. Widespread, commercially available technology that can provide the enemy an unprecedented level of information on friendly forces both greatly challenges and emphasizes OPSEC in facilitating offensive and defensive operations.

**Observable actions, critical indicators, and measures to reduce vulnerabilities:** "Even though we will be in allied territory in our tactical assembly area (TAA), we must expect that special purpose forces (SPF) are going to be operating in high gear. Therefore, OPSEC must be our watchword. We must have aggressive counter-reconnaissance operations of our own and also enlist the support of our Southland allies while in our TAA and operating out of forward area rearming/refueling points (FARPs). We must have protective measures for Q36 or 37 counter-artillery radars and FARPs. Also, I'm concerned with protecting our tactical local area network (TACLAN), both in Southland while in our TAA and, of course, in Northland. Our unsecured Battle Command Net is a vulnerability waiting to happen; however, it may be a fact of life we'll have to live with and accept the risks involved. Nevertheless, take a look to see if there are any possible protective measures we can implement for it. Last, but certainly not least, we have to protect our disposition and intentions, especially

for our main effort, for our deception operation, and for our future actions. Consider using specific tactical deception measures, such as Q36 or 37 mockups and false FARPs, as decoys to reduce the probability of detection and targeting of our real resources. I realize that there is a tradeoff in resources that has to be made for actual and deception operations. This is exacerbated by the fact that we're third in priority with Corps for their deception support. The Chief of Staff and G3 can make decisions on those tradeoffs during your COA analysis, but tell me specifically what those were when you present me the decision brief."

### **EW Considerations**

As most information is processed and transmitted via electronic means, EW is a primary tool that the commander has to deny, disrupt, or degrade the enemy's use of information while protecting his own. Additionally, availability and use of the electromagnetic spectrum have become critical factors in conducting modern military operations. By definition, EW is the commander's capability to influence and control the spectrum within his battlespace.

**Electronic protect (EP) priorities:** "My priorities for EP are the Battle Command Net, principally because it's totally unsecured, Q36 or 37 radars, and our TACLAN. I need you to come back after wargaming the COAs and tell me how much risk we're going to have to accept on the Battle Command Net. Also, look at if and when it might be appropriate to use jamming as an EP measure to screen our operations from enemy signals intelligence (SIGINT) during and after the assault."

**Support needed for EW:** "I know that we're second priority for Corps EW support. Nevertheless, we don't have the resources to reach deep enough to jam the enemy air defense, maneuver, and artillery assets that we need to for setting the conditions for our success both in deep attacks and the close fight. Therefore, we'll have to depend on Corps and EAC support; tell me if our priority for Corps support changes. Likewise, the G2 will need to maintain close contact with Corps to identify our requirements and determine what the threat is deep so EW can be successful."

**Electronic attack (EA):** "My priorities for EA are initially to target SPF and human intelligence (HUMINT) agents while we're in our TAA and operating out of FARP ALPHA. When we begin setting conditions for our assault, EA priorities are air defense (AD) command and control (C<sup>2</sup>) and radars, artillery C<sup>2</sup>, and maneuver C<sup>2</sup>. Once we begin our assault, EA priorities are artillery C<sup>2</sup>, AD C<sup>2</sup> and radars, and then maneuver C<sup>2</sup>. Those will remain my priorities until we complete our mission or until we go into a branch or sequel."

### **Physical Destruction Considerations**

Of all IO techniques, physical attack is perhaps the best understood by military forces. Nevertheless, in IO the use of physical attack is significantly different than maneuver warfare. Critical nodes having an operational effect that directly or indirectly achieves the identified objective(s) are the targets of physical destruction for IO purposes. In many instances, these nodes may not have a directly related combat function and the effect of their destruction may not be immediately discernible or the impact readily assessable.

Targets, maneuver actions, and air defense measures: "During our stay in the TAA, our counter-reconnaissance efforts and security support from our Southland allies should focus on destroying or neutralizing any SPF or HUMINT agents we can locate. Destruction or neutralization of SPF, Army and Division reconnaissance, and HUMINT agents is also paramount during initial entry into Northland. Simultaneously, air defense needs to ensure that enemy aerial ISR assets that attempt to fly near or over our TAA or FARP ALPHA are destroyed. I know that we are expected to have air superiority, but we must have redundancy in ensuring early defeat of his reconnaissance effort. During and subsequent to the assault, we need to ensure we have Corps support in destroying the enemy's airborne jammers, either with air defense or with AI on their bases. I'd like to see them as high-value targets (HVTs). Also during and subsequent to our assault, I want enemy drones and remotely piloted vehicles (RPVs) and their associated ground control stations, AD C<sup>2</sup>, artillery C<sup>2</sup> and counter-mortar/counter-battery (CM/CB) radars, and maneuver C<sup>2</sup> as priority targets. This will be especially critical to setting conditions for our defeat of the enemy's follow-on force: the 25th Tank Division (TD). Of course, successful suppression of enemy air defense (SEAD) against enemy AD C<sup>2</sup> and radars must be a standard for our conduct of deep strikes throughout the operation."

### **PSYOP Considerations**

PSYOP may play the most important role of any IO element in influencing the perceptions and behavior of the enemy and the foreign populace within the commander's battlespace. To cause behavior favorable to the commander's mission success,

PSYOP can provide information directly to enemy soldiers or foreign civilians to dissuade or persuade them or it can provide information for analysis to indirectly influence the enemy's or populace's behavior. PSYOP can be an invaluable contributor to the conduct of civil-military, deception, and public affairs operations to achieve the commander's IO objective(s).

**Priority of effort for attached PSYOP forces:** "While the Division is still in Southland, I want tactical PSYOP forces to concentrate on force protection. First, ensure PSYOP is integrated with CA so that civilian interference with our operations and movements in Southland is eliminated. Second, I want PSYOP to assist in the deception effort aimed at the SPF operating in Southland. Any support PSYOP can add to the deception effort will help protect the FARPs. While in Southland, I want to fully support the Corps and Theater commanders' PSYOP objectives. Simultaneously, we need to specifically capitalize on those efforts and find ways to apply the approved themes in our area of operations (AO) so as to gain collateral tactical benefit for our operation. In particular, target the local Southland population to legitimize our presence and allay the fears of the Southland populace near our TAA. We will have to ask for Corps' help in influencing Northland targets while setting our conditions. I want our IO Cell to identify the high-payoff Northland PSYOP targets in our AO and send them to Corps. Getting our PSYOP targets in the air tasking order (ATO) is a constant battle that I want to win. Once we are on the ground in Northland, I want PSYOP forces up front. Offering the remaining Northland forces an option other than fighting could save combat resources and, most importantly, Division lives. The "stay put" message needs to get out and needs to be credible to keep the Northland civilian populace in their homes. They need to know that staying in place is the only choice their safety. Lastly, I want PSYOP to be involved in the deception effort against the 20th MRD commander. Use all available tactical PSYOP dissemination assets, such as loudspeaker systems, to make the deception more credible."

**Allocation of organic or supporting resources to support PSYOP efforts:** "Our PSYOP efforts will have more credibility when they reinforce applied combat power. I don't expect enemy forces to be persuaded with just logic and words. When we set the conditions for conducting our assaults, we will soften the 20th MRD's perception with our deep strikes and then try to mold it with PSYOP. We will reorient that combination against the 25th TD after we ensure the defeat of any enemy counterattack against our assault to seize the objective by preparing the counterattack force with PSYOP following lethal attack."

### **Public Affairs (PA) Considerations**

The global, real-time reach of a single media representative in the commander's battlespace, the right of the American public to be informed, the benefit of keeping the local populace informed, the need to keep soldiers' families informed, and the duty to inform soldiers all establish the importance of effective PA operations in achieving the commander's IO objective(s). Essentially, either the commander can use his assets and available resources according to his own plan to inform the public on operations in his battlespace, or he can react to the information supplied by others - including the enemy. Of course, the possibility always exists that the commander will have to react to external sources of public information, but it should be according to his own IO plan.

**Effective publications that are dependent on credibility:** "Any information that originates with the Division must be credible. Our entire effort to gain a decisive information advantage depends on that. In fact, lack of credibility in the information we put out may have adverse effects that can ripple through the Corps' and joint task force (JTF)'s information campaign. We will put out the facts at all times. While operating in Southland in our TAA and FARP ALPHA, make sure that we warn the local populace of enemy SPF and agent operations so they can help identify, neutralize, and destroy them. This will also contribute to the JTF's and Corps' overall efforts to maintain the support of our Southland allies. Like PSYOP, I know we have to support the execution of the Corps' and JTF's PA effort. Again, find opportunities to exploit that application for direct collateral benefits to our tactical operation. In addition to getting the information out to the media, we also need to make sure our own soldiers are kept apprised of the situation to head off enemy propaganda and disinformation efforts and prevent rumors. This will be especially critical as we start taking casualties. Any assistance we provide to the local populace should be advertised. Likewise, any incidents of enemy abuses and collateral civilian casualties from enemy attacks should be identified. We should also be able to anticipate and plan for those instances where the Division may cause civilian casualties or be accused of abuses during this operation. Plan for how we will resolve those and get the facts out."

**Early deployment of PA personnel:** "Having our PA people well integrated into the Division IO Cell and planning effort will help ensure we get them integrated into the operation starting in the TAA. Providing credible information will be even more important once we enter Northland. We'll need to have PA support go in on the assault onto the objective to ensure credible information on our operation begins flowing as early as possible."

**Information security practiced at the source:** "Even though we need to keep credible information flowing through the media and to our troops, we've got to protect those critical pieces of information that would go beyond advancing our efforts toward an information advantage and instead contribute to the enemy's effort. That is a delicate balance we need to maintain."

We cannot stifle our best public relations representatives - our soldiers - but everyone must be aware of our EEFI and ensure they're effectively protected. As you develop and analyze COAs, make sure that EEFI are integral to the concept of the operation and evaluated for needed modification. In that way we'll know what information is critical to safeguard and what information we can concentrate on getting out to tell the Division's story and thereby help in telling the Corps' and JTF's story."

### Civil Affairs (CA) Considerations

Through CA, the commander establishes and maintains effective relations between his forces, the local population, and local civil authorities. These relations are critical for providing and obtaining resources vital to the operation, including information on the local and regional situation. Additionally, through effective relations, a commander can establish inclinations in the population and civil authorities to cooperate with his concept of operations.

**Priority of effort for attached CA forces:** "Interface with the host-nation authorities in Southland will probably be the most critical task our CA will need to address during this operation. Support from Southland may be needed in many forms, but from a strict tactical perspective complementing our efforts to find, neutralize, and destroy SPF and enemy agents in Southland will be where we absolutely must have their support. The more assets we have out there to counter the enemy's initial collection and disruption efforts, the better our force protection will be to maintain our freedom of action for deep and close operations. The primary effort for our CA after entering Northland will be the populace vicinity the objective. That concentration is a potential source of interference with our operation. Make sure we aggressively implement a "stay put" policy to keep the civilian populace vicinity the airfield in their homes and away from our operations and main supply route (MSRs). We don't have the assets to support civilian basic needs or casualties so we may have to accept risk there. Let me know if there is anything we can plan on doing for those, such as expecting non-governmental organizations' support. CA can support us by interfacing with Southland and Northland officials to supplement our supplies. I'd like to see that developed during wargaming so we can figure out where and when that might be necessary and whether there will be viable sources in the local area to support us. The G2 should be able to help in locating what supplies might be available in the region. Also, determine what local media means might be available in the area that we can use to complement our PSYOP and PA efforts as well as where and when we might need to use them. Last, as we put in minefields we'll need to warn any local populace to limit collateral civilian casualties. This will be especially important for long-duration mines. Again, figure out when and where we might need to do that; work with PSYOP and PA on getting the information out and advertising our efforts to limit collateral damage and casualties."

### Conclusion

Taking the salient points from the above comprehensive guidance for each individual area, the overall IO guidance that the commander might give for this operation can be summarized in a succinct paragraph:

"During Phase I, I want IO to support force protection by focusing on the defeat of enemy RISTA assets, especially SPF and HUMINT agents, operating against our forces in Southland. My priorities for protection of our critical assets are: the main and tactical CPs, FARPs, Q36 or 37 radars, AH-64s, the Battle Command Net, and our TACLAN, in order. During Phase II, IO will deceive the 20th MRD commander to delay commitment of his local, heavy counterattack force - the 204th TR. My intent is to ensure we have sufficient time to defeat the forces on the objective and begin preparing our positions before facing the 204th TR. I will commit a brigade task force and an attack helicopter battalion to conduct the deception operation. For Phase III, I want to attack the command, control, communications, and intelligence (C<sup>3</sup>I) of his follow-on division, the 25th TD, to force him into an uncoordinated, piecemeal commitment and prevent engagement of our critical assets after we achieve entry into Northland."

**Note:** The authors gratefully acknowledge the editorial contributions of Mr. Leonard G. "Len" Nowak, JB Systems Engineering Support Company, contractor supporting the U.S. Army land information Warfare Activity.

---

#### Endnotes:

1. **FM 101-5, *Staff Organization and Operations***, 31 May 1997, pg B-2. Specific guidance on civil affairs is not included in Appendix B, Commander's Guidance Guidelines; however, considerations identified under the fire support battlefield operating system guidance include "...cultural, religious, historical, and high-density civilian population areas" relative to the protected target list.
2. Draft LIWA Field Support Team (FST) Handbook, Command and Control Warfare (C<sup>2</sup>W), 1 August 1996, pg 3-4.

3. FM 101-5, 5-10, and Primer, Information Operations, 4th Inf Div DAWE, November 1997, pg 11.

4. FM 101-5, pg B-2.

5. **FM 100-6, *Information Operations***, August 1996, pgs 2-3 and 3-0, and Joint Publication No. 3-13, Joint Doctrine for Information Operations, 9 October 1998, pg 1-3.

---